ANNEX 10

ASEAN Defense Ministers' Meeting (ADMM-Plus)

CYBERSECURITY

EXPERTS' WORKING GROUP

ADMM

ASEAN Defence Ministers' Meeting

Developments on ICT's Security @ADMM+Plus EWG on Cyber Security

By: **BGEN JESS LOMEDA (Ret)**
Co-Chair, ADMM+ EWG on CS
Chief, MISS, DND, Philippines

ANNEX 10

SCOPE OF PRESENTATION

- Concept Paper
- Inaugural Meeting at Manila, Philippines
  July 17-19, 2017
- 2nd Meeting at Wellington, New Zealand
  November 1-17, 2017
- Way Ahead:
  - 3rd Meeting at Cebu City, Philippines
    May 16-18, 2018
  - 4th Meting at Auckland, New Zealand
    November 2018

ANNEX 10

ADMM-Plus EWG for Cybersecurity

ASEAN

1. Brunei
2. Cambodia
3. Indonesia
4. LaoPDR
5. Malaysia
6. Myanmar
7. Philippines
8. Singapore
9. Thailand
10. Vietnam

Plus

1. Australia
2. China
3. India
4. Japan
5. New Zealand
6. Republic of Korea
7. Russia
8. United States

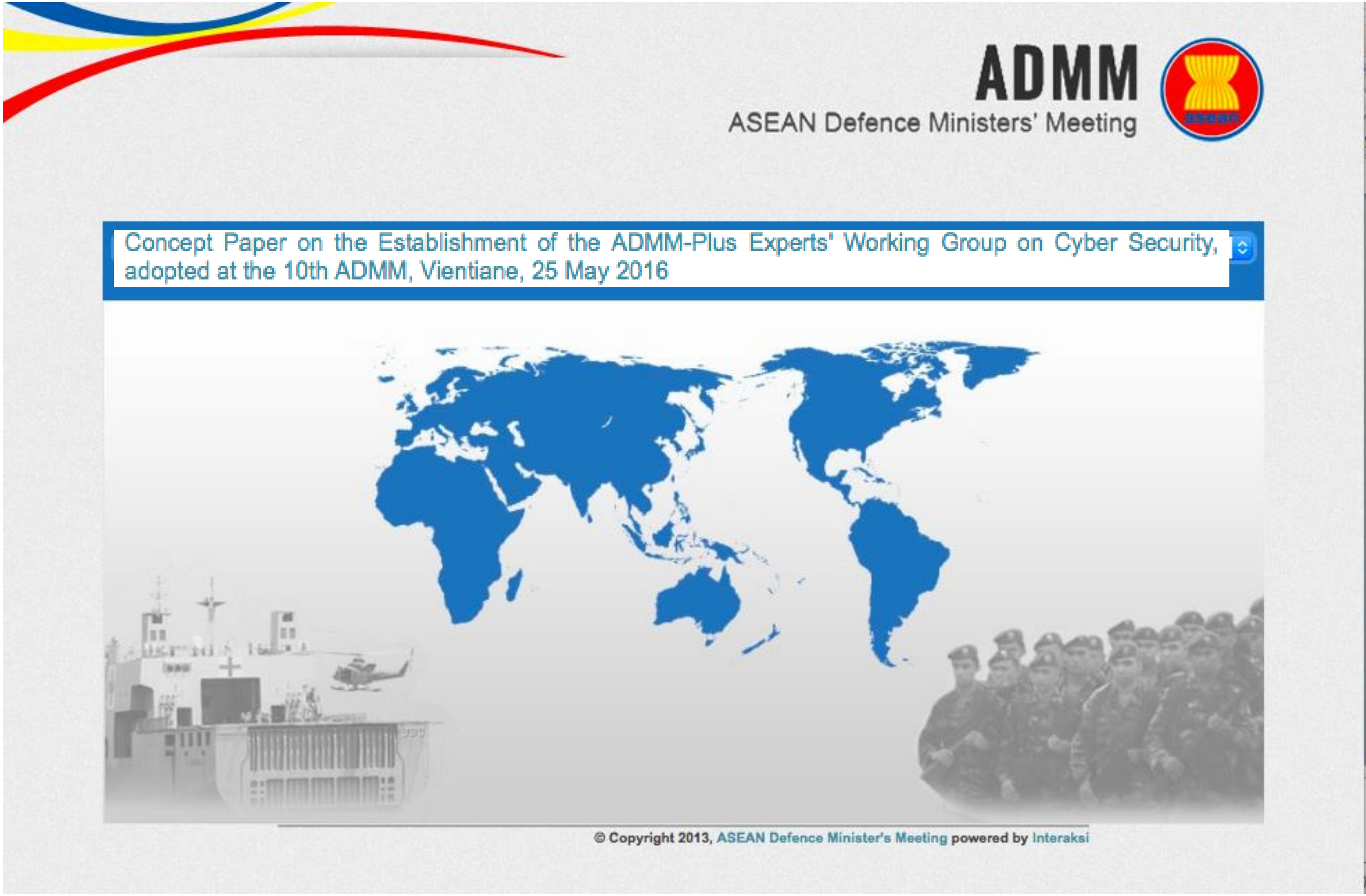
ANNEX 10

ADMM-Plus Experts' Working Groups

1) Humanitarian Assistance and Disaster Relief;
2) Maritime Security;
3) Military Medicine;
4) CounterTerrorism;
5) Peacekeeping Operations;
6) Humanitarian Mine Action; and
7) Cybersecurity, which was only created in May 2016 at Laos.

https://admm.asean.org

ANNEX 10



ADMM

ASEAN Defence Ministers' Meeting

Concept Paper on the Establishment of the ADMM-Plus Experts' Working Group on Cyber Security, adopted at the 10th ADMM, Vientiane, 25 May 2016

© Copyright 2013, ASEAN Defence Minister's Meeting powered by Interaksi

ANNEX 10

Purpose

The establishment of the ADMM-Plus EWG on Cyber Security aims to promote practical and effective cooperation among the ASEAN Member States and Plus Countries **to enhance capacity in protecting the region’s cyberspace and addressing challenges to cyber security**.

ANNEX 10

Objective

1. To **enhance awareness** on cyber security challenges and responsibilities for each nation and the international community to address such challenges;
2. To **leverage capabilities** of each nation in addressing cyber security challenges;
3. To encourage the ASEAN Member States, Plus Countries and the international community to **make common efforts** to protect cyberspace;
4. To **develop cooperative solutions** and initiatives to effectively address cyber security threats; and
5. To **develop appropriate mechanisms** for cooperation among the defence and military establishments of the ADMM-Plus countries and for coordination of military and civilian groups in addressing cyber challenges.

ANNEX 10

Functions

- Implement the ADSOM-Plus and ADMM-Plus decisions, and **provide policy recommendations**.
- Discuss and **suggest specific solutions**, scope and areas of cooperation that would address cyber security challenges in the region, and consistent with the existing cooperation frameworks in ASEAN.

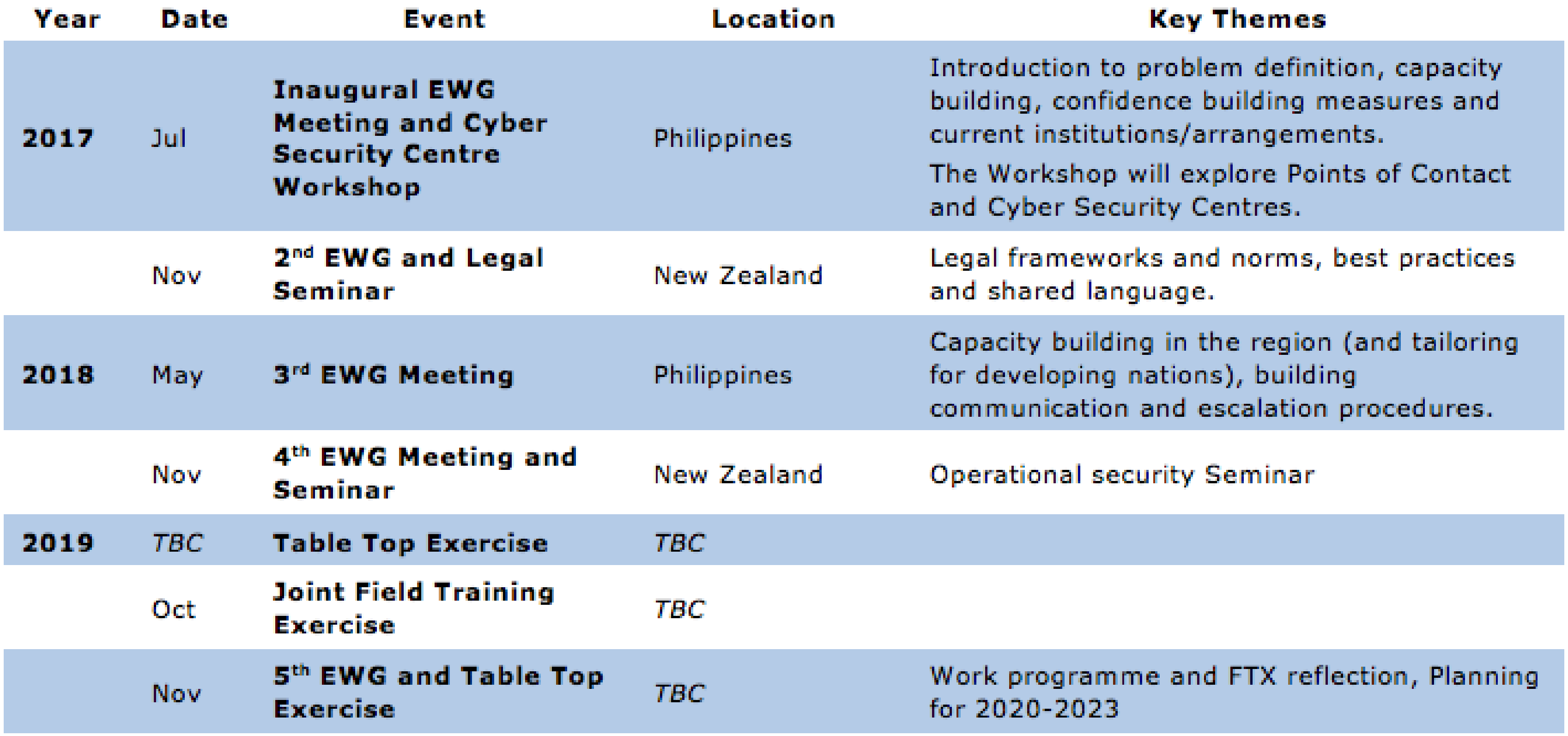
ANNEX 10

Responsibilities

- Discussing various initiatives that would promote cooperation on cyber security and address regional cyber security challenges;
- Crafting a roadmap and **plan of action** which will be implemented upon approval;
- Providing thorough assessment of activities of the EWG, propose necessary adjustments and additions to higher leaders for approval;
- Working closely with Cyber Security Agencies of member countries to ensure that the roadmap, the procedures for consultation and the policy recommendations could address cyber security challenges and are in accordance with respective country's laws;
- Ensuring that the initiatives of the EWG on Cyber Security complement other initiatives of ASEAN on this aspect; and
- **Hosting meetings and conferences, conducting exercises and trainings and preparing reports to higher leaders**.

ANNEX 10

Plan of Action (Road Map)



Year	Date	Event	Location	Key Themes
2017	Jul	**Inaugural EWG Meeting and Cyber Security Centre Workshop**	Philippines	Introduction to problem definition, capacity building, confidence building measures and current institutions/arrangements. The Workshop will explore Points of Contact and Cyber Security Centres.
	Nov	**2nd EWG and Legal Seminar**	New Zealand	Legal frameworks and norms, best practices and shared language.
2018	May	**3rd EWG Meeting**	Philippines	Capacity building in the region (and tailoring for developing nations), building communication and escalation procedures.
	Nov	**4th EWG Meeting and Seminar**	New Zealand	Operational security Seminar
2019	*TBC*	**Table Top Exercise**	*TBC*	
	Oct	**Joint Field Training Exercise**	*TBC*	
	Nov	**5th EWG and Table Top Exercise**	*TBC*	Work programme and FTX reflection, Planning for 2020-2023

ANNEX 10

Scope of Cooperation

The cooperation activities under this EWG will focus only on cyber security issues related to the defense and military sectors. Cooperation within the ambit of the EWG may include:

- Convening of meetings and conferences to **share experiences and information on cybersecurity** and to enhance mutual understanding on related issues.
- Holding of conferences **to develop policies and framework of cooperation on cybersecurity** in accordance with international laws as well as each country's respective laws.
- Undertaking of **exchanges of subject matter and technical experts** for training and sharing of knowledge regarding the matter.
- **Conduct of exercises and trainings** that would enhance each country's capabilities to address cyber security challenges.
- Sharing of appropriate **technologies, equipment and resources** for cyber security.

ANNEX 10

Inaugural Meeting

17-19 July 2017, Manila, Philippines

Agenda : How to attain the objectives?
Establishment of Points-of-Contact

ANNEX 10

PLENARY SESSION

- Panel Discussions:
  - **Mr. Joe Burton** (University of Waikato), SME from New Zealand who discussed about Cyber Security in the Asia Pacific and its Challenges;
  - **BGen Pedro A. Sumayo Jr**., AFP Assistant Deputy Chief-of-Staff for C4S, AJ6, who discussed about Armed Forces of the Philippines (AFP) cyber update.

ANNEX 10

OBJECTIVES

Concept Paper of the ADMM-Plus EWG for Cybersecurity

SYNDICATE #1 (Australia, Brunei, Cambodia, China, India and Indonesia):

1) To enhance **AWARENESS** on cyber security challenges and responsibilities of each nation and the international community to address such challenges;

2) To **LEVERAGE CAPABILITIES** of each nation in addressing cyber security challenges;

SYNDICATE #2 (Japan, LaoPDR, Malaysia and Myanmar):

3) To encourage the ASEAN Member States, Plus Countries and the international community to make **COMMON EFFORTS TO PROTECT CYBERSPACE;**

4) To develop **COOPERATIVE SOLUTIONS AND INITIATIVES** to effectively address cyber security threats; and

SYNDICATE #3 (Russia, Singapore, Thailand, USA and Vietnam):

5) To develop appropriate **MECHANISMS FOR COOPERATION** among the defense and military establishments of the ADMM -Plus countries and for coordination of military and civilian groups in addressing cyber security challenges.

ANNEX 10

SYNDICATE GROUP #1

ASEAN 50 PHILIPPINES 2017

PARTNERING FOR CHANGE, ENGAGING THE WORLD

ASEAN Defense Ministers' Meeting (ADMM-Plus)

CYBERSEC

EXPERTS' WORKING GROUP

ANNEX 10

How to enhance **AWARENESS** on cyber security challenges and responsibilities of each nation and the international community to address such challenges?

- ✓ A venue to share whitepapers and best practices, such as: websites/internet for a.
- ✓ Sharing of government mechanisms and frameworks among member-states in seminars and workshops.
- ✓ Enhance international cooperation and collaboration through multi-lateral meetings.

ANNEX 10

How to **LEVERAGE CAPABILITIES** of each nation in addressing cyber security challenges?

- ✓ Subject Matter Expert Exchanges (SMEEs) and multi-lateral training;
- ✓ Adoption of policies/best practices from success stories of other nations;
- ✓ Establishment of CERTs or CIRTs; and
- ✓ Creation of Cybersecurity Operations Center.

ANNEX 10

SYNDICATE #2

Japan

Lao PDR

Malaysia

Myanmar

ANNEX 10

- How to encourage the ASEAN Member States, Plus Countries and the international community to make common efforts to protect cyberspace?

- How to develop cooperative solutions and initiatives to effectively address cyber security threats?

Friday, January 11, 2019

ANNEX 10

SYNTHESIS

1. Cyberspace

- ICT network
- Culture & Way of Life
- Threats

2. Objective

- How to encourage the ASEAN Members States, Plus Countries and the international community to make common efforts to protect cyberspace.
- How to develop cooperative solutions and initiatives for effectively address cyber security threats..

3. Principle

- Cooperation among nation states
- Rule of law / International Law / sense of Order

4. Common Effort

- Incident Response
- Cyber Security Awareness
- Cyber Security Agency
- Cyber Security Related Laws
- Capacity Building
- Resources

5. Initiatives

- Establishment of Points of Contact
- Cyber Security Related Workshop
- Cyber Threat Information Sharing
- Cyber Security Trainings

ANNEX 10

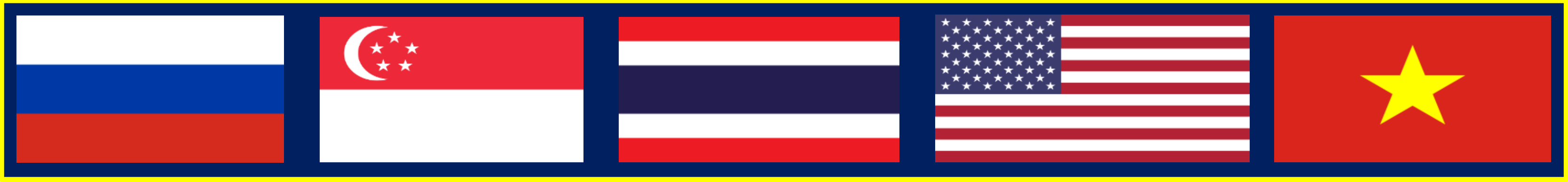
ASEAN 50
PHILIPPINES 2017
PARTNERING FOR CHANGE, ENGAGING THE WORLD

ASEAN Defense Ministers' Meeting (ADMM-Plus)

CYBERSEC

EXPERTS' WORKING GROUP

Syndicate Group 3



ANNEX 10

How to develop appropriate **MECHANISMS** for cooperation among the defense and military establishments of the ADMM - Plus countries and for coordination of military and civilian groups in addressing cyber security challenges?

- ✓ To cultivate trust and understanding among the cyber workforces through experts exchanges and interactions;
- ✓ To conduct Bilateral/Multilateral exercises to enhance coordination; and
- ✓ To have active partnership collaboration on Cybersecurity concerns.

ANNEX 10

ASEAN Defense Ministers' Meeting (ADMM-Plus)

CYBERSECURITY

EXPERTS' WORKING GROUP

POINTS-OF-CONTACT

ANNEX 10

POINTS-OF-CONTACT

ASEAN Member Countries

Country	Contact Person	Name of Office	Address		e-mail address
BRUNEI DARUSSALAM	**AZIZ YAAKUB**	Directorate of Defence Policy	Block D, Level 3, Ministry of Defence, Bolkiah Garrison	abdaziz.yaakub@mindef.gov.bn	(+673)238 6069 / (+673) 822 1208
CAMBODIA	**MGEN KUCHCHANDARA HOEUNG**	-	-	kuchchandara@mod.gov.kh	-
INDONESIA	**IKWAN ACHMADI**	International Cooperation MOD	Merdeka Barat 14 Jakarta	multilateralmod@yahoo.com ikwan.achmadi@kemhan.go.id ikwan93@yahoo.com	(+62)213500428
LAO PDR	**CAPT OUD SIPASIRTH**	ASEAN Political Security Division	Ministry of National Defense, Vientiane	sipasirth.oud@gmail.com	856 20 29806236
MALAYSIA	**COL DR SAYUTHI B JAAFAR**	Cyber Warfare Strategic Branch Defense Intelligence Service Div	Malaysian Armed Forces Headquarters	sayuthi@mod.gov.my	(019)3537796 & 0182090040
MYANMAR	**COL. KO KO OO**	Office of the Chief of Military Security Affairs	OCMSA, May Pyi Taw, Myanmar	kko2O06@gmail.com	594-2044404
PHILIPPINES	**DIR. NEBUCHADNEZZAR S. ALEJANDRINO**	Defense Situation Monitoring Center, Department of National Defense	DND Building, Camp Aguinaldo, Quezon City, Philippines	dsmc_cyber2dnd.gov.ph	(+632)2856364
SINGAPORE	**SLTC JOHN LIOW**	Defence Cyber Organization Collaboration and Defence Relations Department	308 Gombak Drive #05-22 Singapore, 669646	john_liow@mindef.gov.sg	(+65)63075828
THAILAND	**None Indicated**	Director, Office of ASEAN Affairs, Office of Policy and Planning	Sanamchai R, Pranakorn, Bangkok, Thailand	aseanmod.thai@gmail.com	(+662)2252015
VIETNAM	**PHAM VIET TRUNG**	Department of Information Technology	34A Tran Phu, Hanoi	trungpv@mod.gov.vn	(+84)965030358

ANNEX 10

POINTS-OF-CONTACT

ASEAN-PLUS Countries

Country	Contact Person	Name of Office	Address	e-mail address	telephone nr.
AUSTRALIA	**MARK RIFFEL**	Director, Strategic Capabilities	-	mark.riffel@defence.gov.au	-
CHINA	-	-	-	winiter@outlook.com	-
INDIA	**COL HARSH BHATIA**	COL	Room No. 58, Kashmir House, New Delhi	harsh_bhatia@yahoo.com	1123011386
JAPAN	**COL KAZUNOBU AKUTSU**	Japan Embassy in the Philippines	Embassy of Japan in the Philippines 2627 Roxas Blvd, Manila	kazunobu.akutsu@mofa.go.jp	(+63)917-820-1253
NEW ZEALAND	**MICHAEL THOMPSON**	Director (asia), International Branch, Ministry of Defense	Freybera Building, 20 Aitken Street, Wellington	mike.thompson@defence.govt.nz	(+64)44960999
RUSSIAN FEDERATION	**Contacts are in the ASEAN Secretariat and you may contact Military Attache in Jakarta**	General Staff of RF Armed Forces	Moscow	-	-
USA	**PHILIP ROBBINS**	HQ V.S. Pacific Command	Camp HM Smith	philip.robbins@navy.mil	808-798-1554
	LCT JACKY LY	US ASEAN	US Embassy, Jakarta, Indonesia	lytv@state.gov	(62)812 109 4396

ANNEX 10

ASEAN Defense Ministers' Meeting (ADMM-Plus)

CYBERSECURITY EXPERTS' WORKING GROUP

2nd Meeting

15-17 November 2017, Wellington, New Zealand

Agenda : Legal frameworks and norms, best practices and shared language

ANNEX 10

Agenda

Legal Framework

Norms

Best Practices

Shared Language

ANNEX 10

Speakers

- **Charlotte Beaglehole**, Co-Chair and Head of the International Branch of the Ministry of Defense: Welcome Address.
- **Paul Ash**, the Director of the National Cyber Policy Office, Department of the Prime Minister and Cabinet, New Zealand: Cybersecurity in the Defense Context:Today, threats in cyber include risks to life and health.
- **Tim Wood** (SQNLDR), the Director of Defence Legal Services of the New Zealand Defence Force (NZDF): Defence Act of 1990, which highlights the protection of New Zealand's interest and provision of public service.
- **Liis Vihul**, the Chief Executive Officer of Cyber Law International and a member of the Estonian delegations at UN GGE on Information and Telecommunications: Tallinn Manual 2.0.
- **Mike Thompson**, the Director (Asia & US) International Branch at Ministry of Defence: Cyber in Targeting and Law of Armed Conflict (LOAC, the concept of cyber operations has the same legal principle.

ANNEX 10

Syndicate Discussion

- Based on existing international law and norms, what practical initiatives might work in a military context?
- What are possible cyber security CBMs in military context and how might these be established by this EWG in context of the ADMM-Plus given its focus on practical mil-mil cooperation?
- What are the cyber security implications for the work of the other EWGs and how might we contribute to cyber security resilience for them?

ANNEX 10

1st Syndicate Group

- The recognition of disparity between legal and command language, operational constraints. That is why there is a need to delineate operation and **conduct basic discussion of cyber law** before applying it in the military context.
- There are differences in capacity and capability of each country – this result in different understanding of common laws. It was recommended that **workshop of legal offices** be conducted to establish understanding of international law.
- There is a need to delineate national policies and laws before applying international law, and **conduct ASEAN cooperation** instead of bilateral processes.

ANNEX 10

2nd Syndicate Group

- Reiterated on **regular meetings** such as the EWG to be conducted to establish trust and confidentiality among states.
- The **creation of a manual** for the ADMM-Plus such as the Tallinn Manual that shall apply own consensus on the international and national laws.
- Initiatives such as CERTs or **cyber security centers** are established to ensure resilience of cyber infrastructure and for public-private sectors to strengthen their culture and examine security issues on the internet of things.
- **Joint training** such as table top exercises (TTX) and field training exercises (FTX) should also be conducted.

ANNEX 10

3rd Syndicate Group

- Reiterated the need for a **common understanding** most importantly due to the lack of cyber law and disparity among legal frameworks. Due to this, it was recommended that a glossary be created to establish the gap on common understanding.
- Looking at **baseline operational** cyber security behaviors that can be facilitated in rules of engagement and/or its applicability in other EWGs.
- The EWG should accommodate a **technical cooperation** as part of the Confidence Building Measures (CBM).
- The EWG **share strategies** in cyber including domestic laws, reference materials, and adoption of norms and declarations.

ANNEX 10

Country Presentations

- **Brunei Darussalam** reported about the 16th ASEAN Telecommunications and Information Technology Ministers Meeting (TELMIN). The ASEAN TELMIN have launched the ASEAN ICT Masterplan 2020 (AIM 2020) which envisions a “digitally enabled economy that is secure, sustainable, and transformative”.
- **Singapore** briefed the group about the Singapore International Cyber Week (SICW) held last September 2017, which is a five (5) day event where policy makers, though leaders, and experts came together to forge partnerships and exchange discourse on cybersecurity challenges.
- **New Zealand** which discussed about cyber security in the ASEAN Regional Forum and gave details on the ASEAN Secretariat’s report.
- **Philippines** talked about the previous EWG meeting and the way ahead that the next meeting will be in Cebu City, Philippines.

ANNEX 10

ASEAN Defense Ministers' Meeting (ADMM-Plus)

CYBERSECURITY

EXPERTS' WORKING GROUP

3rd Meeting

16-18 May 2018, Cebu Philippines

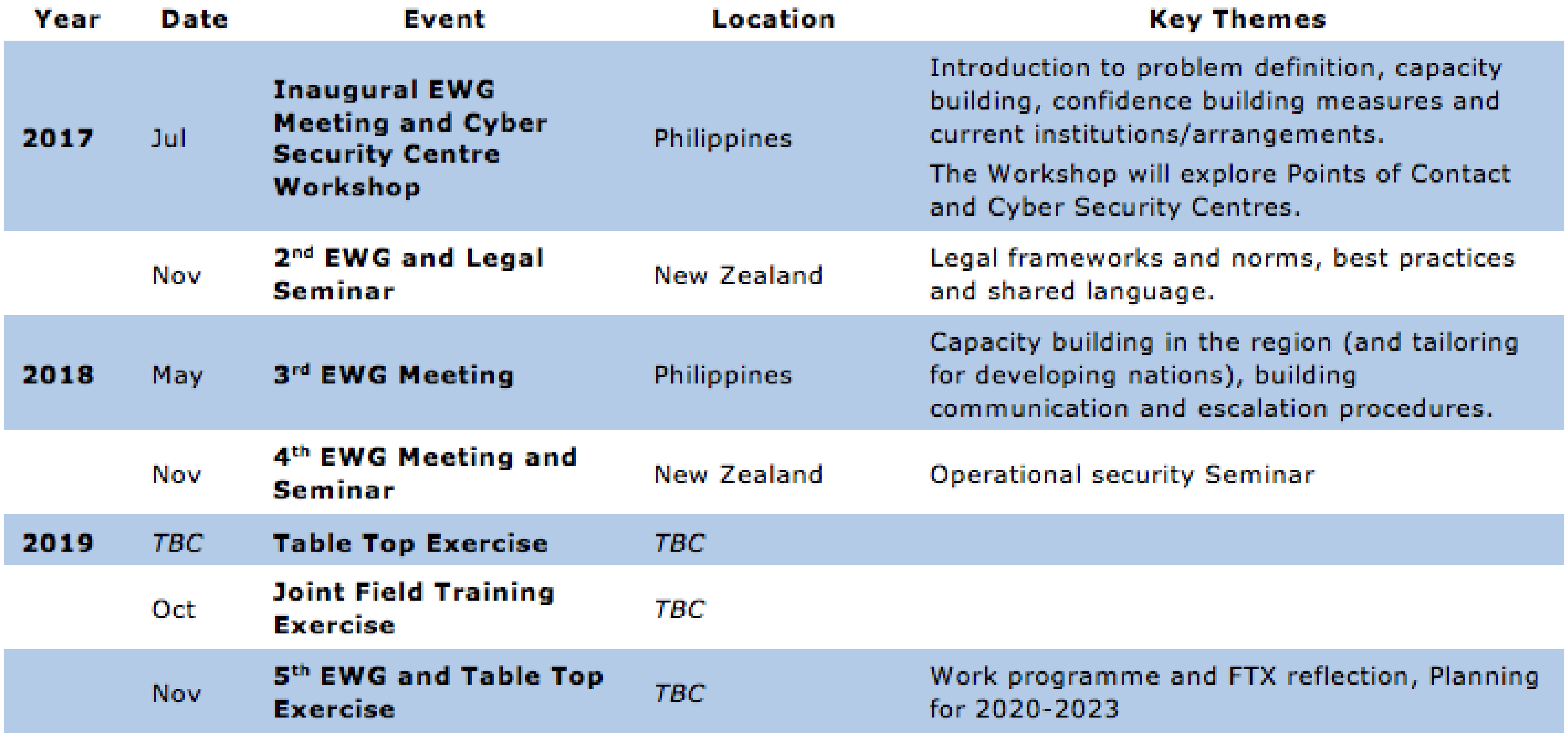
AGENDA :

- Devise a communications plan which guides how cyber security issues are escalated and communicated.

- Compile a glossary of cyber terminology.

ANNEX 10

Plan of Action (Road Map)



Year	Date	Event	Location	Key Themes
2017	Jul	**Inaugural EWG Meeting and Cyber Security Centre Workshop**	Philippines	Introduction to problem definition, capacity building, confidence building measures and current institutions/arrangements. The Workshop will explore Points of Contact and Cyber Security Centres.
	Nov	**2nd EWG and Legal Seminar**	New Zealand	Legal frameworks and norms, best practices and shared language.
2018	May	**3rd EWG Meeting**	Philippines	Capacity building in the region (and tailoring for developing nations), building communication and escalation procedures.
	Nov	**4th EWG Meeting and Seminar**	New Zealand	Operational security Seminar
2019	*TBC*	**Table Top Exercise**	*TBC*	
	Oct	**Joint Field Training Exercise**	*TBC*	
	Nov	**5th EWG and Table Top Exercise**	*TBC*	Work programme and FTX reflection, Planning for 2020-2023

ANNEX 10

Conclusion

With the continuing development of ICTs, the establishment of the EWG on Cyber Security would serve as an essential platform to protect the region's cyberspace and promote cooperation on cyber security.